**3GPP TSG-WG SA2 Meeting #154AH  *S2-230xxxx***

**Online, 16-20 January 2023 (*revision of 1602*)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **4083** | **rev** | **-1** | **Current version:** | **18.0.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Support of network slice replacement  |
|  |  |
| ***Source to WG:*** | ZTE, [LG Electronics, NEC, Ericsson, Lenovo, InterDigital, Apple,Samsung, Nokia, Nokia Shanghai Bell] |
| ***Source to TSG:*** | S2 |
|  |  |
| ***Work item code:*** | eNS\_Ph3 |  | ***Date:*** | 2023-01-09 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | This CR introduce the support of network slice replacement feature as concluded in TR 23.700 41 New Rev in SA2#155: address the following Editor NOTEsEditor's note: Whether both, the PCF and the NSSF options are specified or one of the option is FFS.Editor's note: Whether an S-NSSAI can be replaced with more than one Alternative S-NSSAI is FFS. |
|  |  |
| ***Summary of change:*** | Support of network slice replacement |
| ***--*** |  |
| ***Consequences if not approved:*** | Lack of support of this feature  |
|  |  |
| ***Clauses affected:*** | 3.1, 5.15.x, 5.4.4a, 5.15.1, 5.15.2.1, 5.15.4.1.1,15.4.1.2, 5.15.4.2, 5.15.5.2.2, 5.15.5.3, 6.2.1, 6.2.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ... |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR’s revision history:*** |  |

##

## **FIRST CHANGE**

### 5.15.x Support of Network Slice Replacement

Based on local configuration (e.g. based on trigger from OAM when an S-NSSAI is not available or congested) or based on S-NSSAI availability notification from NSSF, the AMF may determine that a old S-NSSAI is to be replaced with an Alternative S-NSSAI. The NSSF may include Alternative S-NSSA that may be used by AMF to replace the old S-NSSAI. If no Alternative S-NSSAI is received in the notification from the NSSF and the AMF does not locally determine any Alternative S-NSSAI value, the AMF may provide the old S-NSSAI to PCF to retrieve the Alternative S-NSSA(s) for the old S-NSSAI. Whether to interact with PCF is based on AMF configuration. Based on received information from PCF or NSSF, and local configuration, the AMF determines single Alternative S-NSSAI to replace the old S-NSSAI for a UE registered with the old S-NSSAI (i.e. the S-NSSAI is in the UE’s Allowed NSSAI). The Alternative S-NSSAI shall be supported in the current UE Registration Area.

In roaming case if the serving AMF supports the Network Slice Replacement feature, the AMF may subscribe with the NSSF of the VPLMN for notifications when an VPLMN S-NSSAI or HPLMN S-NSSAI needs to be replaced with an Alternative S-NSSAI. The NSSF of the VPLMN shall subscribe with the NSSF of the HPLMN for notifications when an HPLMN S-NSSAI needs to be replaced with an Alternative S-NSSAI

If the UE indicates the support of Network Slice Replacement feature during the UE Registration procedure, and some S-NSSAI needs to be replaced, the AMF provides the Alternative S-NSSAI in the Allowed NSSAI and/or in the Configured NSSAI, if not included yet, and the mapping between S-NSSAI(s) to Alternative S-NSSAI(s) to the UE in UE Configuration Update message as follows:

- for non-roaming UEs, the AMF provides the mapping of old S-NSSAI to the Alternative S-NSSAI to the UE.

- for roaming UEs when the VPLMN S-NSSAI has to be replaced, the AMF provides the mapping of old VPLMN S-NSSAI to the Alternative S-NSSAI to the UE.

- for roaming UEs when the HPLMN S-NSSAI has to be replaced, the AMF provides the mapping of old HPLMN S-NSSAI to the Alternative HPLMN S-NSSAI to the UE.

NOTE 1: The Alternative S-NSSAI or Alternative HPLMN S-NSSAI may be part or not part of the Subscribed S-NSSAI.

NOTE 2: The Slice Replacement is only used when the resource of S-NSSAI cannot be repartitioned

Editor's note: Whether the AMF can send the mapping between S-NSSAI(s) to Alternative S-NSSAI(s) in Registration Accept message is FFS.

The UE may include the Alternative S-NSSAI as part of Requested NSSAI in the RRC Connection Establishment for AMF selection in the NG-RAN.

Editor's note: It is FFS when the UE provides the Alternative S-NSSAI in the RRC Connection Establishment.

During the new PDU Session establishment procedure towards an old S-NSSAI, if the UE is provided with the mapping of old S-NSSAI to the Alternative S-NSSAI, the UE provides both the Alternative S-NSSAI and the old S-NSSAI in the PDU Session Establishment message. When the AMF receives the Alternative S-NSSAI in the PDU Session Establishment message, or when the AMF does not receive Alternative S-NSSAI in the PDU Session Establishment message (i.e. the UE is not provided with the mapping of old S-NSSAI to the Alternative S-NSSAI) and the AMF determines that the requested S-NSSAI is to be replaced with the Alternative S-NSSAI, the AMF includes both the old S-NSSAI and the Alternative S-NSSAI to the SMF. The SMF proceeds with the PDU Session establishment using the Alternative S-NSSAI. The SMF sends the Alternative S-NSSAI to NG-RAN in N2 SM information and to UE in PDU Session Establishment Accept message.

For existing PDU Session associated with an S-NSSAI that is replaced with the Alternative S-NSSAI, the AMF updates the SMF of the PDU Session, e.g. triggering Nsmf\_PDUSession\_UpdateSMContext service operation, that the PDU Session is to be transferred to Alternative S-NSSAI and includes the Alternative S-NSSAI as follows (see details in clause 4.3.5.x of TS 23.502 [3]):

- If the SMF determines that the PDU Session needs to be retained (e.g if the anchor UPF can be reused with the alternative S-NSSAI and SSC mode 1), the SMF sends the Alternative S-NSSAI to the UPF in the N4 message, to the NG-RAN in N2 message and to the UE in N1 message.

- If the SMF determines that the PDU Session needs to be re-established, the SMF sends to the UE either PDU Session Modification Command if the PDU Session is of SSC mode 3, or PDU Session Release if the PDU Session is of SSC mode 2 or SSC mode 1, to trigger the re-establishment of the PDU Session. The UE includes both, the S-NSSAI being replaced and the Alternative S-NSSAI in the PDU Session Establishment message.

## **Next CHANGE**

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**5G VN Group:** A set of UEs using private communication for 5G LAN-type service.

**5G Access Network:** An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network.

**5G Access Stratum-based Time Distribution:** A time synchronization distribution method that is used by an NG-RAN to provide the 5GS time to the UE(s) over the radio interface using procedures specified in TS 38.331 [28].

**5G Core Network:** The core network specified in the present document. It connects to a 5G Access Network.

**5G LAN-Type Service:** A service over the 5G system offering private communication using IP and/or non-IP type communications.

**5G LAN-Virtual Network:** A virtual network over the 5G system capable of supporting 5G LAN-type service.

**5G NSWO:** The 5G NSWO is the capability provided by 5G system and by UE to enable the connection to a WLAN access network using 5GS credentials without registration to 5GS.

**5G QoS Flow or QoS Flow:** The finest granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receive the same forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Providing different QoS forwarding treatment requires separate 5G QoS Flow.

**5G QoS Identifier:** A scalar that is used as a reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a 5G QoS Flow. This may be implemented in the access network by the 5QI referencing node specific parameters that control the QoS forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

**5G System:** 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE.

**5G-BRG:** The 5G-BRG is a 5G-RG defined in BBF.

**5G-CRG:** The 5G-CRG is a 5G-RG specified in DOCSIS MULPI [89].

**5G-RG:** A 5G-RG is a RG capable of connecting to 5GC playing the role of a UE with regard to the 5G core. It supports secure element and exchanges N1 signalling with 5GC. The 5G-RG can be either a 5G-BRG or 5G-CRG.

**Access Traffic Steering:** The procedure that selects an access network for a new data flow and transfers the traffic of this data flow over the selected access network. Access traffic steering is applicable between one 3GPP access and one non-3GPP access.

**Access Traffic Switching:** The procedure that moves all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow. Access traffic switching is applicable between one 3GPP access and one non-3GPP access.

**Access Traffic Splitting:** The procedure that splits the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access and some other traffic of the same data flow is transferred via another access. Access traffic splitting is applicable between one 3GPP access and one non-3GPP access.

**Allowed NSSAI**: Indicating the S-NSSAIs values the UE could use in the Serving PLMN in the current Registration Area.

**Allowed Area:** Area where the UE is allowed to initiate communication as specified in clause 5.3.2.3.

**Alternative S-NSSAI:** Indicating a compatible S-NSSAI for an S-NSSAI in the Allowed NSSAI that the AMF uses to replace an S-NSSAI when the S-NSSAI is not available or congested, as specified in clause 5.15.x.**AMF Region:** An AMF Region consists of one or multiple AMF Sets.

**AMF Set:** An AMF Set consists of some AMFs that serve a given area and Network Slice(s). AMF Set is unique within an AMF Region and it comprises of AMFs that support the same Network Slice(s). Multiple AMF Sets may be defined per AMF Region. The AMF instances in the same AMF Set may be geographically distributed but have access to the same context data.

**Application Identifier:** An identifier that can be mapped to a specific application traffic detection rule.

**AUSF Group ID:** This refers to one or more AUSF instances managing a specific set of SUPIs. An AUSF Group consists of one or multiple AUSF Sets.

**Binding Indication:** Information included by a NF service producer to a NF service consumer in request responses or notifications to convey the scope within which selection/reselection of target NF/NF Services may be performed, or information included by the NF service consumer in requests or subscriptions to convey the scope within which selection/reselection of notification targets or the selection of other service(s) that the NF consumer produces for the same data context may be performed. See clause 6.3.1.0.

**BSF Group ID:** This refers to one or more BSF instances managing a specific set of SUPIs or GPSIs. A BSF Group consists of one or multiple BSF Sets.

**Configured NSSAI:** NSSAI provisioned in the UE applicable to one or more PLMNs.

**CHF Group ID:** This refers to one or more CHF instances managing a specific set of SUPIs.

**Credentials Holder:** Entity which authenticates and authorizes access to an SNPN separate from the Credentials Holder.

**Default UE credentials:** Information configured in the UE to make the UE uniquely identifiable and verifiably secure to perform UE onboarding.

**Default Credentials Server (DCS):** An entity that can perform authentication based on the Default UE credentials or provide means for another entity to perform authentication based on the Default UE credentials.

**Delegated Discovery:** This refers to delegating the discovery and associated selection of NF instances or NF service instances to an SCP.

**Direct Communication:** This refers to the communication between NFs or NF services without using an SCP.

**Disaster Condition:** See definition in TS 22.261 [2].

**Disaster Inbound Roamer:** See definition in TS 22.261 [2].

**Disaster Roaming:** See definition in TS 22.261 [2].

**DN Access Identifier (DNAI):** Identifier of a user plane access to one or more DN(s) where applications are deployed.

**Emergency Registered:** A UE is considered Emergency Registered over an Access Type in a PLMN when registered for emergency services only over this Access Type in this PLMN.

**Endpoint Address:** An address in the format of an IP address or FQDN, which is used to determine the host/authority part of the target URI. This Target URI is used to access an NF service (i.e. to invoke service operations) of an NF service producer or for notifications to an NF service consumer.

**En-gNB:** as defined in TS 37.340 [31].

**Expected UE Behaviour:** Set of parameters provisioned by an external party to 5G network functions on the foreseen or expected UE behaviour, see clause 5.20.

**Fixed Network Residential Gateway:** A Fixed Network RG (FN-RG) is a RG that it does not support N1 signalling and it is not 5GC capable.

**Fixed Network Broadband Residential Gateway:** A Fixed Network RG (FN-BRG) is a FN-RG specified in BBF TR‑124 [90].

**Fixed Network Cable Residential Gateway:** A Fixed Network Cable RG (FN-CRG) is a FN-RG with cable modem specified in DOCSIS MULPI [89].

**Forbidden Area:** An area where the UE is not allowed to initiate communication as specified in clause 5.3.2.3.

**GBR QoS Flow:** A QoS Flow using the GBR resource type or the Delay-critical GBR resource type and requiring guaranteed flow bit rate.

**Group ID for Network Selection (GIN):** An identifier used during SNPN selection to enhance the likelihood of selecting a preferred SNPN that supports a Default Credentials Server or a Credentials Holder.

**(g)PTP-based Time Distribution:** a method to distribute timing among entities in a (g)PTP domain using PTP messages generated by a GM (in the case the GM is external to 5GS) or by 5GS (in the case the 5GS acts as a GM for a given (g)PTP domain). Possible dependencies between (g)PTP-based Time Distribution and 5G Access Stratum-based Time Distribution are described in clause 5.27.1. The synchronization process is described in clause 5.27.1 and follows the applicable profiles of IEEE Std 802.1AS [104] or IEEE Std 1588 [126].

**Home Network Public Key Identifier:** An identifier used to indicate which public/private key pair is used for SUPI protection and de-concealment of the SUCI as specified in TS 23.003 [19].

**IAB-donor:** This is a NG-RAN node that supports Integrated access and backhaul (IAB) feature and provides connection to the core network to IAB-nodes. It supports the CU function of the CU/DU architecture for IAB defined in TS 38.401 [42].

**IAB-node:** A relay node that supports wireless in-band and out-of-band relaying of NR access traffic via NR Uu backhaul links. It supports the UE function and the DU function of the CU/DU architecture for IAB defined in TS 38.401 [42].

**Indirect Communication:** This refers to the communication between NFs or NF services via an SCP.

**Initial Registration:** UE registration in RM-DEREGISTERED state as specified in clause 5.3.2.

**Intermediate SMF (I-SMF):** An SMF that is inserted to support a PDU session as the UE is located in an area which cannot be controlled by the original SMF because the UPF(s) belong to a different SMF Service Area.

**Local Area Data Network:** a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.

**Local Break Out (LBO):** Roaming scenario for a PDU Session where the PDU Session Anchor and its controlling SMF are located in the serving PLMN (VPLMN).

**LTE-M:** a 3GPP RAT type Identifier used in the Core Network only, which is a sub-type of E-UTRA RAT type, and defined to identify in the Core Network the E-UTRA when used by a UE indicating Category M.

**MA PDU Session:** A PDU Session that provides a PDU connectivity service, which can use one access network at a time, or simultaneously one 3GPP access network and one non-3GPP access network.

**Mobility Pattern:** Network concept of determining within the AMF the UE mobility parameters as specified in clause 5.3.2.4.

**Mobility Registration Update:** UE re-registration when entering new TA outside the TAI List as specified in clause 5.3.2.

**MPS-subscribed UE:** A UE having a USIM with MPS subscription.

**Multi-USIM UE:** A UE with multiple USIMs, capable of maintaining a separate registration state with a PLMN for each USIM at least over 3GPP Access and supporting one or more of the features described in clause 5.38.

**NB-IoT UE Priority:** Numerical value used by the NG-RAN to prioritise between different UEs accessing via NB-IoT.

**NGAP UE association:** The logical per UE association between a 5G-AN node and an AMF.

**NGAP UE-TNLA-binding:** The binding between a NGAP UE association and a specific TNL association for a given UE.

**Network Function:** A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces.

NOTE 1: A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure.

**Network Instance**: Information identifying a domain. Used by the UPF for traffic detection and routing.

**Network Slice:** A logical network that provides specific network capabilities and network characteristics.

**Network Slice instance:** A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice.

**Non-GBR QoS Flow:** A QoS Flow using the Non-GBR resource type and not requiring guaranteed flow bit rate.

**NSI ID:** an identifier for identifying the Core Network part of a Network Slice instance when multiple Network Slice instances of the same Network Slice are deployed, and there is a need to differentiate between them in the 5GC.

**NF instance:** an identifiable instance of the NF.

**NF service:** a functionality exposed by a NF through a service-based interface and consumed by other authorized NFs.

**NF service instance:** an identifiable instance of the NF service.

**NF service operation:** An elementary unit a NF service is composed of.

**NF Service Set:** A group of interchangeable NF service instances of the same service type within an NF instance. The NF service instances in the same NF Service Set have access to the same context data.

**NF Set:** A group of interchangeable NF instances of the same type, supporting the same services and the same Network Slice(s). The NF instances in the same NF Set may be geographically distributed but have access to the same context data.

**NG-RAN:** A radio access network that supports one or more of the following options with the common characteristics that it connects to 5GC:

1) Standalone New Radio.

2) New Radio is the anchor with E-UTRA extensions.

3) Standalone E-UTRA.

4) E-UTRA is the anchor with New Radio extensions.

**Non-Allowed Area:** Area where the UE is allowed to initiate Registration procedure but no other communication as specified in clause 5.3.2.3.

Non-Public Network: See definition in TS 22.261 [2].

**Non-Seamless Non-3GPP offload:** The offload of user plane traffic via non-3GPP access without traversing either N3IWF/TNGF or UPF.

**Non-Seamless WLAN offload:** Non-Seamless Non-3GPP offload when the non-3GPP access network is WLAN.

**Onboarding Network:** Either a PLMN enabling Remote Provisioning for a registered UE, or an Onboarding SNPN.

**Onboarding Standalone Non-Public Network:** An SNPN providing Onboarding access and enabling Remote Provisioning for a UE registered for Onboarding as specified in clause 4.2.2.2.4 of TS 23.502 [3].

**PCF Group ID:** This refers to one or more PCF instances managing a specific set of SUPIs. A PCF Group consists of one or multiple PCF Sets.

**Pending NSSAI:** NSSAI provided by the Serving PLMN during a Registration procedure, indicating the S-NSSAI(s) for which the network slice-specific authentication and authorization procedure is pending.

**PDU Connectivity Service:** A service that provides exchange of PDUs between a UE and a Data Network.

**PDU Session:** Association between the UE and a Data Network that provides a PDU connectivity service.

**PDU Session Type:** The type of PDU Session which can be IPv4, IPv6, IPv4v6, Ethernet or Unstructured.

**Periodic Registration Update:** UE re-registration at expiry of periodic registration timer as specified in clause 5.3.2.

**PLMN with Disaster Condition:** A PLMN to which a Disaster Condition applies.

**Pre-configured 5QI:** Pre-defined QoS characteristics configured in the AN and 5GC and referenced via a non-standardized 5QI value.

**Private communication:** See definition in TS 22.261 [2].

**Provisioning Server:** Entity that provisions network credentials and other data in the UE to enable SNPN access.

**PTP domain:** As defined in IEEE Std 1588 [126].

**Public network integrated NPN:** A non-public network deployed with the support of a PLMN.

**(Radio) Access Network**: See 5G Access Network.

**RAT type:** Identifies the transmission technology used in the access network for both 3GPP accesses and non-3GPP Accesses, for example, NR, NB-IOT, Untrusted Non-3GPP, Trusted Non-3GPP, Trusted IEEE 802.11 Non-3GPP access, Wireline, Wireline-Cable, Wireline-BBF, etc.

**NR RedCap:** a 3GPP RAT type Identifier used in the Core Network only, which is a sub-type of NR RAT type, and defined to identify in the Core Network the NR when used by a UE indicating NR RedCap.

**Requested NSSAI:** NSSAI provided by the UE to the Serving PLMN during registration.

**Residential Gateway:** The Residential Gateway (RG) is a device providing, for example voice, data, broadcast video, video on demand, to other devices in customer premises.

**Routing Binding Indication:** Information included in a request or notification and that can be used by the SCP for discovery and associated selection to of a suitable target. See clauses 6.3.1.0 and 7.1.2

**Routing Indicator:** Indicator that allows together with SUCI/SUPI Home Network Identifier to route network signalling to AUSF and UDM instances capable to serve the subscriber.

**SCP Domain:** A configured group of one or more SCP(s) and zero or more NF instances(s). An SCP within the group can communicate with any NF instance or SCP within the same group directly, i.e. without passing through an intermediate SCP.

**SNPN-enabled UE:** A UE configured to use stand-alone Non-Public Networks.

**SNPN access mode:** A UE operating in SNPN access mode only selects stand-alone Non-Public Networks over Uu.

**Service based interface:** It represents how a set of services is provided/exposed by a given NF.

**Service Continuity:** The uninterrupted user experience of a service, including the cases where the IP address and/or anchoring point change.

**Service Data Flow Filter:** A set of packet flow header parameter values/ranges used to identify one or more of the (IP or Ethernet) packet flows constituting a Service Data Flow.

**Service Data Flow Template:** The set of Service Data Flow filters in a policy rule or an application identifier in a policy rule referring to an application detection filter, required for defining a Service Data Flow.

**Session Continuity:** The continuity of a PDU Session. For PDU Session of IPv4 or IPv6 or IPv4v6 type "session continuity" implies that the IP address is preserved for the lifetime of the PDU Session.

**SMF Service Area:** The collection of UPF Service Areas of all UPFs which can be controlled by one SMF.

**SNPN ID:** PLMN ID and NID identifying an SNPN.

**Stand-alone Non-Public Network:** A non-public network not relying on network functions provided by a PLMN

**Subscribed S-NSSAI**: S-NSSAI based on subscriber information, which a UE is subscribed to use in a PLMN

**Subscription Owner Standalone Non-Public Network:** A Standalone Non-Public Network owning the subscription of a UE and providing subscription data to the UE via a Provisioning Server during the onboarding procedure.

**Survival Time:** The time that an application consuming a communication service may continue without an anticipated message.

NOTE 2: Taken from clause 3.1 of TS 22.261 [2].

**Target NSSAI:** NSSAI provided by the Serving PLMN to the NG-RAN to cause the NG-RAN to attempt to steer the UE to a cell supporting the Network Slices identified by the S-NSSAIs in this NSSAI. See clause 5.3.4.3.3 for more details.

**Time Sensitive Communication (TSC):** A communication service that supports deterministic communication (i.e. which ensures a maximum delay) and/or isochronous communication with high reliability and availability. It is about providing packet transport with QoS characteristics such as bounds on latency, loss, and reliability, where end systems and relay/transmit nodes may or may not be strictly synchronized.

**TSN working domain:** Synchronization domain for a localized set of devices collaborating on a specific task or work function in a TSN network, corresponding to a gPTP domain defined in IEEE 802.1AS [104].

**UDM Group ID:** This refers to one or more UDM instances managing a specific set of SUPIs. An UDM Group consists of one or multiple UDM Sets.

**UDR Group ID:** This refers to one or more UDR instances managing a specific set of SUPIs. An UDR Group consists of one or multiple UDR Sets.

**UE-DS-TT Residence Time:** The time taken within the UE and DS-TT to forward a packet, i.e. between the ingress of the UE and the DS-TT port in the DL direction, or between the DS-TT port and the egress of the UE in the UL direction. UE-DS-TT Residence Time is provided at the time of PDU Session Establishment by the UE to the network.

NOTE 3: UE-DS-TT Residence Time is the same for uplink and downlink traffic and applies to all QoS Flows.

**UPF Service Area**: An area consisting of one or more TA(s) within which PDU Session associated with the UPF can be served by (R)AN nodes via a N3 interface between the (R)AN and the UPF without need to add a new UPF in between or to remove/re-allocate the UPF.

**Uplink Classifier:** UPF functionality that aims at diverting Uplink traffic, based on filter rules provided by SMF, towards Data Network.

**WB-E-UTRA:** In the RAN, WB-E-UTRA is the part of E-UTRA that excludes NB-IoT. In the Core Network, WB-E-UTRA also excludes LTE-M.

**Wireline 5G Access Network:** The Wireline 5G Access Network (W-5GAN) is a wireline AN that connects to a 5GC via N2 and N3 reference points. The W-5GAN can be either a W-5GBAN or W-5GCAN.

**Wireline 5G Cable Access Network:** The Wireline 5G Cable Access Network (W-5GCAN) is the Access Network defined in CableLabs.

**Wireline BBF Access Network:** The Wireline 5G BBF Access Network (W-5GBAN) is the Access Network defined in BBF.

**Wireline Access Gateway Function (W-AGF):** The Wireline Access Gateway Function (W-AGF) is a Network function in W-5GAN that provides connectivity to the 5G Core to 5G-RG and FN-RG.

NOTE 4: If one AUSF/PCF/UDR/UDM group consists of multiple AUSF/PCF/UDR/UDM Sets, AUSF/PCF/UDR/UDM instance from different Set may be selected to serve the same UE. The temporary data which is not shared across different Sets may be lost, e.g. the event subscriptions stored at one UDM instance are lost if another UDM instance from different Set is selected and no data shared across the UDM Sets.

## **Next CHANGE**

### 5.4.4a UE MM Core Network Capability handling

The UE MM Core Network Capability is split into the S1 UE network capability (mostly for E-UTRAN access related core network parameters) and the UE 5GMM Core Network Capability (mostly to include other UE capabilities related to 5GCN or interworking with EPS) as defined in TS 24.501 [47] and contains non radio-related capabilities, e.g. the NAS security algorithms, etc. The S1 UE network capability is transferred between all CN nodes at AMF to AMF, AMF to MME, MME to MME, and MME to AMF changes. The UE 5GMM Core Network Capability is transferred only at AMF to AMF changes.

In order to ensure that the UE MM Core Network Capability information stored in the AMF is up to date (e.g. to handle the situation when the USIM is moved into a different device while out of coverage, and the old device did not send the Detach message; and the cases of inter-RAT Registration Area Update), the UE shall send the UE MM Core Network Capability information to the AMF during the Initial Registration and Mobility Registration Update procedure within the NAS message.

The AMF shall store always the latest UE MM Core Network Capability received from the UE. Any UE MM Core Network Capability that an AMF receives from an old AMF/MME is replaced when the UE provides the UE MM Core Network Capability with Registration signalling.

If the UE's UE MM Core Network Capability information changes (in either CM-CONNECTED or in CM-IDLE state), the UE shall perform a Mobility Registration Update procedure when it next returns to NG-RAN coverage. See clause 4.2.2 of TS 23.502 [3].

The UE shall indicate in the UE 5GMM Core Network Capability if the UE supports:

- Attach in EPC with Request type "Handover" in PDN CONNECTIVITY Request message (clause 5.3.2.1 of TS 23.401 [26]).

- EPC NAS.

- SMS over NAS.

- LCS.

- 5G SRVCC from NG-RAN to UTRAN, as specified in TS 23.216 [88].

- Radio Capabilities Signalling optimisation (RACS).

- Network Slice-Specific Authentication and Authorization.

- Network Slice Replacement as described in clause 5.15.x.

- Parameters in Supported Network Behaviour for 5G CIoT as described in clause 5.31.2.

- Receiving WUS Assistance Information (E-UTRA) see clause 5.4.9..

- Paging Subgrouping Support Indication (NR) see clause 5.4.12.

- CAG, see clause 5.30.3.3.

- Subscription-based restrictions to simultaneous registration of network slices (see clause 5.15.12).

- Support of NSAG (see clause 5.15.14).

- Minimization of Service Interruption (MINT), as described in clause 5.40.

If a UE operating two or more USIMs, supports and intends to use one or more Multi-USIM features (see clause 5.38) in a PLMN for a USIM, it shall indicate in the UE 5GMM Core Network Capability for this USIM in this PLMN that it supports these one or more Multi-USIM features with the following indications:

- Connection Release Supported.

- Paging Cause Indication for Voice Service Supported.

- Reject Paging Request Supported.

- Paging Restriction Supported.

Otherwise, the UE with the capabilities of Multi-USIM features but does not intend to use them shall not indicate support of these one or more Multi-USIM features.

A UE not operating two or more USIMs shall indicate the Multi-USIM features are not supported.

NOTE: It is not necessary for a UE operating two or more USIMs to use Multi-USIM features with all USIMs.

## **Next CHANGE**

### 5.15.1 General

A Network Slice instance is defined within a PLMN or within an SNPN and shall include:

- the Core Network Control Plane and User Plane Network Functions, as described in clause 4.2,

and, in the serving PLMN, at least one of the following:

- the NG-RAN described in TS 38.300 [27];

- the N3IWF or TNGF functions to the non-3GPP Access Network described in clause 4.2.8.2 or the TWIF functions to the trusted WLAN in the case of support of N5CW devices described in clause 4.2.8.5;

- the W-AGF function to the Wireline Access Network described in clause 4.2.8.4.

The 5G System deployed in a PLMN shall always support the procedures, information and configurations specified to support Network Slice instance selection in the present document, TS 23.502 [3] and TS 23.503 [45].

Network slicing support for roaming is described in clause 5.15.6.

Network slices may differ for supported features and network functions optimisations, in which case such Network Slices may have e.g. different S-NSSAIs with different Slice/Service Types (see clause 5.15.2.1). The operator can deploy multiple Network Slices delivering exactly the same features but for different groups of UEs, e.g. as they deliver a different committed service and/or because they are dedicated to a customer, in which case such Network Slices may have e.g. different S-NSSAIs with the same Slice/Service Type but different Slice Differentiators (see clause 5.15.2.1).

The network may serve a single UE with one or more Network Slice instances simultaneously via a 5G-AN regardless of the access type(s) over which the UE is registered (i.e. 3GPP Access and/or N3GPP Access). The AMF instance serving the UE logically belongs to each of the Network Slice instances serving the UE, i.e. this AMF instance is common to the Network Slice instances serving a UE.

NOTE 1: Number of simultaneous connection of Network Slice instances per UE is limited by the number of S-NSSAIs in the Requested/Allowed NSSAI as described in clause 5.15.2.1.

NOTE 2: In this Release of the specification it is assumed that in any (home or visited) PLMN it is always possible to select an AMF that can serve any combination of S-NSSAIs that will be provided as an Allowed NSSAI.

The selection of the set of Network Slice instances for a UE is triggered by the first contacted AMF in a Registration procedure normally by interacting with the NSSF, and can lead to a change of AMF. This is further described in clause 5.15.5.

A PDU Session belongs to one and only one specific Network Slice instance per PLMN. Different Network Slice instances do not share a PDU Session, though different Network Slice instances may have slice-specific PDU Sessions using the same DNN.

During the Handover procedure the source AMF selects a target AMF by interacting with the NRF as specified in clause 6.3.5.

Network Slice-Specific Authentication and Authorization (NSSAA) enables Network Slice specific authentication as described in clause 5.15.10.

Network Slice Admission Control (NSAC) controls the number of registered UEs per network slice and the number of PDU Sessions per network slice as described in clause 5.15.11.

Support of subscription-based restrictions to simultaneous registration of network slices uses Network Slice Simultaneous Registration Group (NSSRG) information to enable control of which Network Slices that can be registered simultaneously by a UE as described in clause 5.15.12.

Support of data rate limitation per Network Slice for a UE enables enforcement of Maximum Bit Rate per Network Slice for a UE as described in clause 5.15.13.

Support of Network Slice Replacement is described in clause 5.15.x.

### 5.15.2 Identification and selection of a Network Slice: the S-NSSAI and the NSSAI

#### 5.15.2.1 General

An S-NSSAI identifies a Network Slice.

An S-NSSAI is comprised of:

- A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services;

- A Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

An S-NSSAI can have standard values (i.e. such S-NSSAI is only comprised of an SST with a standardised SST value, see clause 5.15.2.2, and no SD) or non-standard values (i.e. such S-NSSAI is comprised of either both an SST and an SD or only an SST without a standardised SST value and no SD). An S-NSSAI with a non-standard value identifies a single Network Slice within the PLMN with which it is associated. An S-NSSAI with a non-standard value shall not be used by the UE in access stratum procedures in any PLMN other than the one to which the S-NSSAI is associated.

The S-NSSAIs in the NSSP of the URSP rules (see clause 6.6.2 of TS 23.503 [45]) and in the Subscribed S-NSSAIs (see clause 5.15.3) contain only HPLMN S-NSSAI values.

The S-NSSAIs in the Configured NSSAI, the Allowed NSSAI (see clause 5.15.4.1), the Requested NSSAI (see clause 5.15.5.2.1), the Rejected S-NSSAIs contain only values from the Serving PLMN. The Serving PLMN can be the HPLMN or a VPLMN.

The S-NSSAI(s) in the PDU Session Establishment contain one Serving PLMN S-NSSAI value and in addition may contain a corresponding HPLMN S-NSSAI value to which this first value is mapped (see clause 5.15.5.3). Further information for slice replacement is described in clause 5.15.x.

The optional mapping of Serving PLMN S-NSSAIs to HPLMN S-NSSAIs contains Serving PLMN S-NSSAI values and corresponding mapped HPLMN S-NSSAI values.

The NSSAI is a collection of S-NSSAIs. An NSSAI may be a Configured NSSAI, a Requested NSSAI or an Allowed NSSAI. There can be at most eight S-NSSAIs in Allowed and Requested NSSAIs sent in signalling messages between the UE and the Network. The Requested NSSAI signalled by the UE to the network allows the network to select the Serving AMF, Network Slice(s) and Network Slice instance(s) for this UE, as specified in clause 5.15.5.

Based on the operator's operational or deployment needs, a Network Slice instance can be associated with one or more S-NSSAIs, and an S-NSSAI can be associated with one or more Network Slice instances. Multiple Network Slice instances associated with the same S-NSSAI may be deployed in the same or in different Tracking Areas. When multiple Network Slice instances associated with the same S-NSSAI are deployed in the same Tracking Areas, the AMF instance serving the UE may logically belong to (i.e. be common to) more than one Network Slice instance associated with this S-NSSAI.

In a PLMN, when an S-NSSAI is associated with more than one Network Slice instance, one of these Network Slice instances, as a result of the Network Slice instance selection procedure defined in clause 5.15.5, serves a UE that is allowed to use this S-NSSAI. For any S-NSSAI, the network may at any one time serve the UE with only one Network Slice instance associated with this S-NSSAI until cases occur where e.g. this Network Slice instance is no longer valid in a given Registration Area, or a change in UE's Allowed NSSAI occurs, etc. In such cases, procedures mentioned in clause 5.15.5.2.2 or clause 5.15.5.2.3 apply.

Based on the Requested NSSAI (if any) and the Subscription Information, the 5GC is responsible for selection of a Network Slice instance(s) to serve a UE including the 5GC Control Plane and User Plane Network Functions corresponding to this Network Slice instance(s). The Subscription Information may contain restrictions to the simultaneous registration of network slices. This is provided to the serving AMF as part of the UE subscription, in the form of Network Slice Simultaneous Registration Group (NSSRG) information (see clause 5.15.12).

The (R)AN may use Requested NSSAI in access stratum signalling to handle the UE Control Plane connection before the 5GC informs the (R)AN of the Allowed NSSAI. The Requested NSSAI is used by the RAN for AMF selection, as described in clause 6.3.5. The UE shall not include the Requested NSSAI in the RRC Resume when the UE asks to resume the RRC connection and is CM-CONNECTED with RRC Inactive state.

When a UE is successfully registered over an Access Type, the CN informs the (R)AN by providing the Allowed NSSAI for the corresponding Access Type.

NOTE: The details of how the RAN uses NSSAI information are described in TS 38.300 [27].

## **Next CHANGE**

### 5.15.4 UE NSSAI configuration and NSSAI storage aspects

#### 5.15.4.1 General

##### 5.15.4.1.1 UE Network Slice configuration

The Network Slice configuration information contains one or more Configured NSSAI(s). A Configured NSSAI may either be configured by a Serving PLMN and apply to the Serving PLMN, or may be a Default Configured NSSAI configured by the HPLMN and that applies to any PLMNs for which no specific Configured NSSAI has been provided to the UE. There is at most one Configured NSSAI per PLMN.

NOTE 1: The value(s) used in the Default Configured NSSAI are expected to be commonly decided by all roaming partners, e.g. by the use of values standardized by 3GPP or other bodies.

The Default Configured NSSAI, if it is configured in the UE, is used by the UE in a Serving PLMN only if the UE has no Configured NSSAI for the Serving PLMN.

The Configured NSSAI of a PLMN may include S-NSSAIs that have standard values or PLMN-specific values.

The Configured NSSAI for the Serving PLMN includes the S-NSSAI values which can be used in the Serving PLMN and may be associated with mapping of each S-NSSAI of the Configured NSSAI to one or more corresponding HPLMN S-NSSAI values.

A UE subscription may contain Network Slice Simultaneous Registration Group (NSSRG) information. If so, the UE configuration is performed as described in clause 5.15.12.2.

The UE may be pre-configured with the Default Configured NSSAI. The UE may be provisioned/updated with the Default Configured NSSAI, determined by the UDM in the HPLMN, using the UE Parameters Update via UDM Control Plane procedure defined in clause 4.20 of TS 23.502 [3]. Each S-NSSAI in the Default Configured NSSAI may have a corresponding S-NSSAI as part of the Subscribed S-NSSAI(s). Consequently, if the Subscribed S-NSSAI(s) which are also present in the Default Configured NSSAI are updated the UDM should update the Default Configured NSSAI in the UE.

In the HPLMN, the S-NSSAIs in the Configured NSSAI provided as described in clause 5.15.4.2, at the time when they are provided to the UE, shall match the Subscribed S-NSSAIs for the UE. When the Subscribed S-NSSAI(s) are updated (i.e. some existing S-NSSAIs are removed and/or some new S-NSSAIs are added) and one or more are applicable to the Serving PLMN the UE is registered in, as described in clause 5.15.3, or when the associated mapping is updated the AMF shall update the UE with the Configured NSSAI for the Serving PLMN and/or Allowed NSSAI and/or the associated mapping to HPLMN S-NSSAIs (see clause 5.15.4.2). When there is the need to update the Allowed NSSAI, the AMF shall provide the UE with the new Allowed NSSAI and the associated mapping to HPLMN S-NSSAIs, unless the AMF cannot determine the new Allowed NSSAI (e.g. all S-NSSAIs in the old Allowed NSSAI have been removed from the Subscribed S-NSSAIs), in which case the AMF shall not send any Allowed NSSAI to the UE but indicate to the UE to perform a Registration procedure. If the UE is in a CM-IDLE state, the AMF may trigger Network Triggered Service Request or wait until the UE is in a CM-CONNECTED state as described in clause 4.2.4.2, TS 23.502 [3].

When providing a Requested NSSAI to the network upon registration, the UE in a given PLMN only includes and uses S-NSSAIs applying to this PLMN. The mapping of S-NSSAIs of the Requested NSSAI to HPLMN S-NSSAIs may also be provided (see clause 5.15.4.1.2 for when this is needed). The S-NSSAIs in the Requested NSSAI are part of the Configured and/or Allowed NSSAIs applicable for this PLMN, when they are available. If the UE has received NSSRG information together with the Configured NSSAI, it only includes in the Requested NSSAI S-NSSAIs that all share a common NSSRG. If no Configured NSSAI and Allowed NSSAI for the PLMN are available, the S-NSSAIs in the Requested NSSAI correspond to the Default Configured NSSAI, if configured in the UE. Upon successful completion of a UE's Registration procedure over an Access Type, the UE obtains from the AMF an Allowed NSSAI for this Access Type, which includes one or more S-NSSAIs and, if needed (see clause 5.15.4.1.2 for when this is needed), their mapping to the HPLMN S-NSSAIs. These S-NSSAIs are valid for the current Registration Area and Access Type provided by the AMF the UE has registered with and can be used simultaneously by the UE (up to the maximum number of simultaneous Network Slice instances or PDU Sessions).

The UE might also obtain one or more rejected S-NSSAIs with cause and validity of rejection from the AMF. An S-NSSAI may be rejected:

- for the entire PLMN; or

- for the current Registration Area.

While it remains RM-REGISTERED in the PLMN and regardless of the Access Type, the UE shall not re-attempt to register to an S-NSSAI rejected for the entire PLMN until this rejected S-NSSAI is deleted as specified below.

While it remains RM-REGISTERED in the PLMN, the UE shall not re-attempt to register to an S-NSSAI rejected in the current Registration Area until it moves out of the current Registration Area.

NOTE 2: The details and more cases of S-NSSAI rejection are described in TS 24.501 [47].

S-NSSAIs that the UE provides in the Requested NSSAI which are neither in the Allowed NSSAI nor provided as a rejected S-NSSAI, shall, by the UE, not be regarded as rejected, i.e. the UE may request to register these S-NSSAIs again next time the UE sends a Requested NSSAI.

The UE stores (S-)NSSAIs as follows:

- When provisioned with a Configured NSSAI for a PLMN and/or a mapping of Configured NSSAI to HPLMN S-NSSAIs and possibly NSSRG information for each S-NSSAI in the Configured NSSAI (if applicable and supported by the UE), or when requested to remove the configuration due to network slicing subscription change, the UE shall:

- replace any stored (old) Configured NSSAI for this PLMN with the new Configured NSSAI for this PLMN (if applicable); and

- delete any stored associated mapping of this old Configured NSSAI for this PLMN to HPLMN S-NSSAIs and, if present and applicable, store the mapping of Configured NSSAI to HPLMN S-NSSAIs; and

- delete any stored associated NSSRG information for each S-NSSAI of the Configured NSSAI and, if present, store the associated NSSRG information for each S-NSSAI of the Configured NSSAI; and

- delete any stored rejected S-NSSAI for this PLMN;

- keep the received Configured NSSAI for a PLMN (if applicable) and associated mapping to HPLMN S-NSSAIs (if applicable) and associated NSSRG information for each S-NSSAI of the Configured NSSAI (if applicable and supported by the UE) stored in the UE, even when registering in another PLMN, until a new Configured NSSAI for this PLMN and/or associated mapping are provisioned in the UE, or until the network slicing subscription changes, as described in clause 5.15.4.2. The number of Configured NSSAIs and associated mapping to be kept stored in the UE for PLMNs other than the HPLMN is up to UE implementation. A UE shall at least be capable of storing a Configured NSSAI for the serving PLMN including any necessary mapping of the Configured NSSAI for the Serving PLMN to HPLMN S-NSSAIs and the Default Configured NSSAI.

- The Allowed NSSAI received in a Registration Accept message or a UE Configuration Update Command applies to a PLMN when at least a TAI of this PLMN is included in the RA/TAI list included in this Registration Accept message or UE Configuration Update Command. If the UE Configuration Update Command contains an Allowed NSSAI but not a TAI List, then the last received RA/TAI list applies for the decision on which PLMN(s) the Allowed NSSAI is applicable. If received, the Allowed NSSAI for a PLMN and Access Type and any associated mapping of this Allowed NSSAI to HPLMN S-NSSAIs shall be stored in the UE. The UE should store this Allowed NSSAI and any associated mapping of this Allowed NSSAI to HPLMN S-NSSAIs also when the UE is turned off, or until the network slicing subscription changes, as described in clause 5.15.4.2:

NOTE 3: Whether the UE stores the Allowed NSSAI and any associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs also when the UE is turned off is left to UE implementation.

- When a new Allowed NSSAI for a PLMN and any associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs are received over an Access Type, the UE shall:

- replace any stored (old) Allowed NSSAI and any associated mapping for these PLMN and Access Type with this new Allowed NSSAI; and

- delete any stored associated mapping of this old Allowed NSSAI for this PLMN to HPLMN S-NSSAIs and, if present, store the associated mapping of this new Allowed NSSAI to HPLMN S-NSSAIs;

- If received, an S-NSSAI rejected for the entire PLMN shall be stored in the UE while RM-REGISTERED in this PLMN regardless of the Access Type or until it is deleted.

- If received, an S-NSSAI rejected for the current Registration Area shall be stored in the UE while RM-REGISTERED until the UE moves out of the current Registration Area or until the S-NSSAI is deleted.

NOTE 4: The storage aspects of rejected S-NSSAIs are described in TS 24.501 [47].

- If received, the Pending NSSAI shall be stored in the UE as described in TS 24.501 [47].

- If received, the mapping of old S-NSSAI to the Alternative S-NSSAI shall be stored in the UE as described in TS 24.501 [47].

##### 5.15.4.1.2 Mapping of S-NSSAIs values in the Allowed NSSAI and in the Requested NSSAI to the S-NSSAIs values used in the HPLMN

One or more S-NSSAIs in an Allowed NSSAI provided to the UE can have values which are not part of the UE's current Network Slice configuration information for the Serving PLMN. In this case, the network provides the Allowed NSSAI together with the mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN. This mapping information allows the UE to associate Applications to S-NSSAIs of the HPLMN as per NSSP of the URSP rules or as per the UE Local Configuration (if available), as defined in clause 6.1.2.2.1 of TS 23.503 [45] and to the corresponding S-NSSAI from the Allowed NSSAI.

In roaming case, the UE may need to provide the mapping of S-NSSAIs values in the Requested NSSAI to the corresponding S-NSSAI values used in the HPLMN. These values are found in the mapping previously received from the Serving PLMN of the S-NSSAIs of the Configured NSSAI for the Serving PLMN or of the S-NSSAIs of the Allowed NSSAI for the Serving PLMN and Access Type to the corresponding S-NSSAIs values used in the HPLMN.

#### 5.15.4.2 Update of UE Network Slice configuration

At any time, the AMF may provide the UE with a new Configured NSSAI for the Serving PLMN, associated with mapping of the Configured NSSAI to HPLMN S-NSSAIs as specified in clause 5.15.4.1. The Configured NSSAI for the Serving PLMN and the mapping information is either determined in the AMF (if based on configuration, the AMF is allowed to determine the Network Slice configuration for the whole PLMN) or by the NSSF. The AMF provides an updated Configured NSSAI as specified in clause 4.2.4 of TS 23.502 [3], UE Configuration Update procedure.

The AMF shall provide the UE with NSSRG information alongside the Configured NSSAI if NSSRG information is included in the subscription information received from the UDM and if the UE has indicated support for the feature as part of the registration request, see clause 5.15.12.

The AMF may provide the UE with the mapping of old S-NSSAI to the Alternative S-NSSAI if the UE has indicated support for the feature as part of the registration request, see clause 5.15.x.

If the HPLMN performs the configuration update of a UE registered in the HPLMN (e.g. due to a change in the Subscribed S-NSSAI(s) or due to a change of NSSRG information), this results in updates to the Configured NSSAI for the HPLMN and, if applicable, NSSRG information for each S-NSSAI of the Configured NSSAI. Updates to the Allowed NSSAI and/or, if present, to the associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs are also possible if the configuration update affects S-NSSAI(s) in the current Allowed NSSAI.

If the VPLMN performs the configuration update of a UE registered in the VPLMN (e.g. due to a change in the Subscribed S-NSSAI(s), the associated mapping is updated, or due to a change of NSSRG information), this results in updates to the Configured NSSAI for the Serving PLMN and/or to the associated mapping of the Configured NSSAI for the Serving PLMN to HPLMN S-NSSAIs and, if applicable, NSSRG information for each S-NSSAI of the Configured NSSAI. Updates to the Allowed NSSAI and/or to the associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs are also possible if the configuration update affects S-NSSAI(s) in the current Allowed NSSAI.

A UE for which the Configured NSSAI for the Serving PLMN has been updated as described in clause 5.15.4.1 and has been requested to perform a Registration procedure, shall initiate a Registration procedure to receive a new valid Allowed NSSAI (see clause 5.15.5.2.2).

When the subscribed S-NSSAIs change, a UDR flag is set in the HPLMN to make sure the current PLMN (or, if the UE was not reachable, the next serving PLMN) is informed by the UDM that the subscription data for network slicing has changed. The AMF, when it receives the indication from the UDM subscription has changed, indicates the UE that subscription has changed and uses any updated subscription information from the UDM to update the UE. Once the AMF updates the UE and obtains an acknowledgment from the UE, the AMF informs the UDM that the configuration update was successful and the UDM clears the flag in the UDR. If the UE is in a CM-IDLE state, the AMF may trigger Network Triggered Service Request or wait until the UE is in a CM-CONNECTED state as described in clause 4.2.4.2, TS 23.502 [3].

If the UE receives indication from the AMF that Network Slicing subscription has changed, the UE locally deletes the network slicing information it has for all PLMNs, except the Default Configured NSSAI (if present). It also updates the current PLMN network slicing configuration information with any received values from the AMF.

The update of URSP rules (which include the NSSP), if necessary at any time, is described in TS 23.503 [45].

## **Next CHANGE**

##### 5.15.5.2.2 Modification of the Set of Network Slice(s) for a UE

The set of Network Slices for a UE can be changed at any time while the UE is registered with a network, and may be initiated by the network, or by the UE, under certain conditions as described below.

The network, based on local policies, subscription changes and/or UE mobility and/or UE Dispersion data classification, operational reasons (e.g. a Network Slice instance is no longer available or load level information or service experience for a Network Slice or network slice instance provided by the NWDAF), may change the set of Network Slice(s) to which the UE is registered and provide the UE with a new Registration Area and/or Allowed NSSAI and the mapping of this Allowed NSSAI to HPLMN S-NSSAIs, for each Access Type over which the UE is registered. In addition, the network may provide the Configured NSSAI for the Serving PLMN, the associated mapping information, and the rejected S-NSSAIs. The network may perform such a change over each Access Type during a Registration procedure or trigger a notification towards the UE of the change of the Network Slices using a UE Configuration Update procedure as specified in clause 4.2.4 of TS 23.502 [3]. The new Allowed NSSAI(s) and the mapping to HPLMN S-NSSAIs are determined as described in clause 5.15.5.2.1 (an AMF Re-allocation may be needed). The AMF provides the UE with:

- an indication that the acknowledgement from UE is required;

- Configured NSSAI for the Serving PLMN (if required), rejected S-NSSAI(s) (if required) and TAI list, and

- the new Allowed NSSAI with the associated mapping of Allowed NSSAI for each Access Type (as applicable) unless the AMF cannot determine the new Allowed NSSAI (e.g. all S-NSSAIs in the old Allowed NSSAI have been removed from the Subscribed S-NSSAIs).

 Furthermore:

- If the changes to the Allowed NSSAI require the UE to perform immediately a Registration procedure because they affect the existing connectivity to AMF (e.g. the new S-NSSAIs require a separate AMF that cannot be determined by the current serving AMF, or the AMF cannot determine the Allowed NSSAI) or due to AMF local policies also when the changes does not affect the existing connectivity to AMF:

- The serving AMF indicates to the UE the need for the UE to perform a Registration procedure without including the GUAMI or 5G-S-TMSI in the access stratum signalling after entering CM-IDLE state. The AMF shall release the NAS signalling connection to the UE to allow to enter CM-IDLE after receiving the acknowledgement from UE.

- When the UE receives indications to perform a Registration procedure without including the GUAMI or 5G-S-TMSI in the access stratum signalling after entering CM-IDLE state, then:

- The UE deletes any stored (old) Allowed NSSAI and associated mapping as well as any (old) rejected S-NSSAI.

- The UE shall initiate a Registration procedure with the registration type Mobility Registration Update after the UE enters CM-IDLE state as specified in as described in step 4 of clause 4.2.4.2 of TS 23.502 [3]. The UE shall include a Requested NSSAI (as described in clause 5.15.5.2.1) with the associated mapping of Requested NSSAI in the Registration Request message. Also, the UE shall include, subject to the conditions set out in clause 5.15.9, a Requested NSSAI in access stratum signalling but no GUAMI.

- If the AMF determines that the S-NSSAI in the Allowed NSSAI is replaced with Alternative S-NSSAI, the AMF provides the mapping of old S-NSSAI to the Alternative S-NSSAI to the UE (as described in clause 5.15.x).

If there is an established PDU Session associated with emergency services, then the serving AMF indicates to the UE the need for the UE to perform a Registration procedure but does not release the NAS signalling connection to the UE. The UE performs the Registration procedure only after the release of the PDU Session used for the emergency services.

In addition to sending the new Allowed NSSAI to the UE, when a Network Slice used for a one or multiple PDU Sessions is no longer available for a UE, the following applies:

- If the Network Slice becomes no longer available under the same AMF and the Network Slice Replacement is not used (e.g. due to UE subscription change), the AMF indicates to the SMF(s) which PDU Session ID(s) corresponding to the relevant S-NSSAI shall be released. SMF releases the PDU Session according to clause 4.3.4.2 of TS 23.502 [3]. If the Network Slice Replacement is used, the AMF performs Network Slice Replacement as described in clause 5.15.x.

- If the Network Slice becomes no longer available upon a change of AMF (e.g. due to Registration Area change), the new AMF indicates to the old AMF that the PDU Session(s) corresponding to the relevant S-NSSAI shall be released. The old AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the new AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status in the Registration Accept message.

The UE uses either the URSP rules (which includes the NSSP) or the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45] to determine whether ongoing traffic can be routed over existing PDU Sessions belonging to other Network Slices or establish new PDU Session(s) associated with same/other Network Slice.

In order to change the set of S-NSSAIs the UE is registered to over an Access Type, the UE shall initiate a Registration procedure over this Access Type as specified in clause 5.15.5.2.1.

If, for an established PDU Session:

- none of the values of the S-NSSAIs of the HPLMN in the mapping of the Requested NSSAI to S-NSSAIs of the HPLMN included in the Registration Request matches the S-NSSAI of the HPLMN associated with the PDU Session; or

- none of the values of the S-NSSAIs in the Requested NSSAI matches the value of the S-NSSAI of HPLMN associated with the PDU Session and the mapping of the Requested NSSAI to S-NSSAIs of the HPLMN is not included in the Registration Request,

the network shall release this PDU Session as follows.

- the AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status from the AMF.

A change of the set of S-NSSAIs (whether UE or Network initiated) to which the UE is registered may, subject to operator policy, lead to AMF change, as described in clause 5.15.5.2.1.

## **Next CHANGE**

#### 5.15.5.3 Establishing a PDU Session in a Network Slice

The PDU Session Establishment in a Network Slice instance to a DN allows data transmission in a Network Slice instance. A PDU Session is associated to an S-NSSAI and a DNN. A UE that is registered in a PLMN over an Access Type and has obtained a corresponding Allowed NSSAI, shall indicate in the PDU Session Establishment procedure the S-NSSAI according to the NSSP in the URSP rules or according to the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45], and, if available, the DNN the PDU Session is related to. The UE includes the appropriate S-NSSAI from this Allowed NSSAI and, if mapping of the Allowed NSSAI to HPLMN S-NSSAIs was provided, an S-NSSAI with the corresponding value from this mapping.

If the UE cannot determine any S-NSSAI after performing the association of the application to a PDU Session according to clause 6.1.2.2.1 of TS 23.503 [45], the UE shall not indicate any S-NSSAI in the PDU Session Establishment procedure.

The network (HPLMN) may provision the UE with Network Slice selection policy (NSSP) as part of the URSP rules, see clause 6.6.2 of TS 23.503 [45]. When the Subscription Information contains more than one S-NSSAI and the network wants to control/modify the UE usage of those S-NSSAIs, then the network provisions/updates the UE with NSSP as part of the URSP rules. When the Subscription Information contains only one S-NSSAI, the network needs not provision the UE with NSSP as part of the URSP rules. The NSSP rules associate an application with one or more HPLMN S-NSSAIs. A default rule which matches all applications to a HPLMN S-NSSAI may also be included.

The UE shall store and use the URSP rules, including the NSSP, as described in TS 23.503 [45]. When a UE application associated with a specific S-NSSAI requests data transmission:

- if the UE has one or more PDU Sessions established corresponding to the specific S-NSSAI, the UE routes the user data of this application in one of these PDU Sessions, unless other conditions in the UE prohibit the use of these PDU Sessions. If the application provides a DNN, then the UE considers also this DNN to determine which PDU Session to use. This is further described in clause 6.6.2 of TS 23.503 [45].

- If the UE does not have a PDU Session established with this specific S-NSSAI, the UE requests a new PDU Session corresponding to this S-NSSAI and with the DNN that may be provided by the application. In order for the RAN to select a proper resource for supporting network slicing in the RAN, RAN needs to be aware of the Network Slices used by the UE. This is further described in clause 6.6.2 of TS 23.503 [45].

If the AMF is not able to determine the appropriate NRF to query for the S-NSSAI provided by the UE, the AMF may query the NSSF with this specific S-NSSAI, location information, PLMN ID of the SUPI. The NSSF determines and returns the appropriate NRF to be used to select NFs/services within the selected Network Slice instance. The NSSF may also return an NSI ID to be used to select NFs within the selected Network Slice instance to use for this S-NSSAI.

The AMF or NSSF may select a Network Slice instance based on load level and/or Observe Service Experience and/or Dispersion analytics from NWDAF.

The IP address or FQDN of the NSSF is locally configured in the AMF.

SMF discovery and selection within the selected Network Slice instance is initiated by the AMF when a SM message to establish a PDU Session is received from the UE. The appropriate NRF is used to assist the discovery and selection tasks of the required network functions for the selected Network Slice instance.

The AMF queries the appropriate NRF to select an SMF in a Network Slice instance based on S-NSSAI, DNN, NSI-ID (if available) and other information e.g. UE subscription and local operator policies, when the UE triggers PDU Session Establishment. The selected SMF establishes a PDU Session based on S-NSSAI and DNN.

When the AMF belongs to multiple Network Slice instances, based on configuration, the AMF may use an NRF at the appropriate level for the SMF selection.

For further details on the SMF selection, refer to clause 4.3.2.2.3 of TS 23.502 [3].

When a PDU Session for a given S-NSSAI is established using a specific Network Slice instance, the CN provides to the (R)AN the S-NSSAI corresponding to this Network Slice instance to enable the RAN to perform access specific functions.

The UE shall not perform PDU Session handover from one Access Type to another if the S-NSSAI of the PDU Session is not included in the Allowed NSSAI of the target Access Type.

The AMF may perform Network Slice Replacement for the PDU Session as described in clause 5.15.x.

## **Next CHANGE**

### 6.2.1 AMF

The Access and Mobility Management function (AMF) includes the following functionality. Some or all of the AMF functionalities may be supported in a single instance of an AMF:

- Termination of RAN CP interface (N2).

- Termination of NAS (N1), NAS ciphering and integrity protection.

- Registration management.

- Connection management.

- Reachability management.

- Mobility Management.

- Lawful intercept (for AMF events and interface to LI System).

- Provide transport for SM messages between UE and SMF.

- Transparent proxy for routing SM messages.

- Access Authentication.

- Access Authorization.

- Provide transport for SMS messages between UE and SMSF.

- Security Anchor Functionality (SEAF) as specified in TS 33.501 [29].

- Location Services management for regulatory services.

- Provide transport for Location Services messages between UE and LMF as well as between RAN and LMF.

- EPS Bearer ID allocation for interworking with EPS.

- UE mobility event notification.

- S-NSSAIs per TA mapping notification.

- Support for Control Plane CIoT 5GS Optimisation.

- Support for User Plane CIoT 5GS Optimisation.

- Support for restriction of use of Enhanced Coverage.

- Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters).

- Support for Network Slice-Specific Authentication and Authorization.

- Support for charging.

NOTE 1: Regardless of the number of Network functions, there is only one NAS interface instance per access network between the UE and the CN, terminated at one of the Network functions that implements at least NAS security and Mobility Management.

In addition to the functionalities of the AMF described above, the AMF may include the following functionality to support non-3GPP access networks:

- Support of N2 interface with N3IWF/TNGF. Over this interface, some information (e.g. 3GPP Cell Identification) and procedures (e.g. Handover related) defined over 3GPP access may not apply, and non-3GPP access specific information may be applied that do not apply to 3GPP accesses.

- Support of NAS signalling with a UE over N3IWF/TNGF. Some procedures supported by NAS signalling over 3GPP access may be not applicable to untrusted non-3GPP (e.g. Paging) access.

- Support of authentication of UEs connected over N3IWF/TNGF.

- Management of mobility, authentication, and separate security context state(s) of a UE connected via a non-3GPP access or connected via a 3GPP access and a non-3GPP access simultaneously.

- Support as described in clause 5.3.2.3 a co-ordinated RM management context valid over a 3GPP access and a Non 3GPP access.

- Support as described in clause 5.3.3.4 dedicated CM management contexts for the UE for connectivity over non-3GPP access.

NOTE 2: Not all of the functionalities are required to be supported in an instance of a Network Slice.

In addition to the functionalities of the AMF described above, the AMF may include policy related functionalities as described in clause 6.2.8 of TS 23.503 [45].

The AMF uses the N14 interface for AMF re-allocation and AMF to AMF information transfer. This interface may be either intra-PLMN or inter-PLMN (e.g. in the case of inter-PLMN mobility).

In addition to the functionality of the AMF described above, the AMF may include the following functionality to support monitoring in roaming scenarios:

- Normalization of reports according to roaming agreements between VPLMN and HPLMN (e.g. change the location granularity in a report from cell level to a level that is appropriate for the HPLMN); and

- Generation of charging/accounting information for Monitoring Event Reports that are sent to the HPLMN.

In addition to the functionality of the AMF described above, the AMF may provide support for Network Slice restriction and Network Slice instance restriction based on NWDAF analytics.

In addition to the functionalities of the AMF described above, the AMF may provide support for the Disaster Roaming as described in clause 5.40.

In addition to the functionalities of the AMF described above, the AMF may also include following functionalities to support Network Slice Admission Control:

- Support of NSAC for maximum number of UEs as defined in clauses 5.15.11.1 and 5.15.11.3.

In addition to the functionality of the AMF described above, the AMF may include the following functionality to support SNPNs:

- Support for Onboarding of UEs for SNPNs.

In addition to the functionalities of the AMF described above, the AMF may also include following functionalities to support satellite backhaul:

- Support for reporting satellite backhaul category (i.e. GEO, MEO, LEO or OTHERSAT) and its modification based on AMF local configuration to SMF as defined in clause 5.8.2.15.

In addition to the functionalities of the AMF described above, the AMF may also include functionalities to support Network Slice Replacement as described in clause 5.15.x.

## **Next CHANGE**

### 6.2.2 SMF

The Session Management function (SMF) includes the following functionality. Some or all of the SMF functionalities may be supported in a single instance of a SMF:

- Session Management e.g. Session Establishment, modify and release, including tunnel maintain between UPF and AN node.

- UE IP address allocation & management (including optional Authorization). The UE IP address may be received from a UPF or from an external data network.

- DHCPv4 (server and client) and DHCPv6 (server and client) functions.

- Functionality to respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests based on local cache information for the Ethernet PDUs. The SMF responds to the ARP and / or the IPv6 Neighbour Solicitation Request by providing the MAC address corresponding to the IP address sent in the request.

- Selection and control of UP function, including controlling the UPF to proxy ARP or IPv6 Neighbour Discovery, or to forward all ARP/IPv6 Neighbour Solicitation traffic to the SMF, for Ethernet PDU Sessions.

- Configures traffic steering at UPF to route traffic to proper destination.

- 5G VN group management, e.g. maintain the topology of the involved PSA UPFs, establish and release the N19 tunnels between PSA UPFs, configure traffic forwarding at UPF to apply local switching, N6-based forwarding or N19-based forwarding.

- Termination of interfaces towards Policy control functions.

- Lawful intercept (for SM events and interface to LI System).

- Support for charging.

- Control and coordination of charging data collection at UPF.

- Termination of SM parts of NAS messages.

- Downlink Data Notification.

- Initiator of AN specific SM information, sent via AMF over N2 to AN.

- Determine SSC mode of a session.

- Support for Control Plane CIoT 5GS Optimisation.

- Support of header compression.

- Act as I-SMF in deployments where I-SMF can be inserted, removed and relocated.

- Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters).

- Support P-CSCF discovery for IMS services.

- Act as V-SMF with following roaming functionalities:

- Handle local enforcement to apply QoS SLAs (VPLMN).

- Charging (VPLMN).

- Lawful intercept (in VPLMN for SM events and interface to LI System).

- Support for interaction with external DN for transport of signalling for PDU Session authentication/authorization by external DN.

- Instructs UPF and NG-RAN to perform redundant transmission on N3/N9 interfaces.

NOTE: Not all of the functionalities are required to be supported in an instance of a Network Slice.

In addition to the functionalities of the SMF described above, the SMF may include policy related functionalities as described in clause 6.2.2 of TS 23.503 [45].

In addition to the functionality of the SMF described above, the SMF may include the following functionality to support monitoring in roaming scenarios:

- Normalization of reports according to roaming agreements between VPLMN and HPLMN; and

- Generation of charging information for Monitoring Event Reports that are sent to the HPLMN.

The SMF may also include following functionalities to support Edge Computing enhancements (further defined in TS 23.548 [130]):

- Selection of EASDF and provision of its address to the UE as the DNS Server for the PDU session;

- Usage of EASDF services as defined in TS 23.548 [130];

- For supporting the Application Layer Architecture defined in TS 23.558 [134]: Provision and updates of ECS Address Configuration Information to the UE.

The SMF and SMF+ PGW-C may also include following functionalities to support Network Slice Admission Control:

- Support of NSAC for maximum number of PDU sessions as defined in clauses 5.15.11.2, 5.15.11.3 and 5.15.11.5.

- Support of NSAC for maximum number of UEs as defined in clauses 5.15.11.3 and 5.15.11.5.

In addition to the functionalities of the SMF described above, the SMF may also include functionalities to support Network Slice Replacement as described in clause 5.15.x.

## **END of CHANGES**